6. How do you create, schedule, and manage scans in Nessus?

📌 Creating, Scheduling, and Managing Scans in Nessus

Nessus is a **powerful vulnerability scanner** that allows you to **create, schedule, and manage security scans** to detect weaknesses in networks, applications, and systems. Below is a **step-by-step guide** to help you **master scanning in Nessus**. 🚀

🔹 1. Creating a New Scan

To start scanning, follow these steps:

🛠️ Steps to Create a Scan:

1️⃣ **Login to Nessus:** Open your browser and go to `https://localhost:8834`
2️⃣ Click on **"Scans"** in the left menu
3️⃣ Click **"New Scan"**
4️⃣ Choose a **Scan Template** (see below for details)
5️⃣ Enter **Scan Name**, **Description**, and **Target Hosts (IP/domain names)**
6️⃣ Configure **Scan Settings** (e.g., speed, authentication, network policy)
7️⃣ Click **"Save"** or **"Launch"** to start scanning immediately

🔍 Choosing the Right Scan Template

Scan Type	Description
🔹 **Basic Network Scan**	General vulnerability scan for detecting weaknesses in systems.
🔹 **Advanced Scan**	Customizable scan for fine-tuning settings.
🔹 **Credentialed Scan**	Uses login credentials to analyze internal vulnerabilities.
🔹 **Web Application Scan**	Identifies OWASP Top 10 web security issues.
🔹 **Malware Scan**	Detects malicious code and backdoors on the system.
🔹 **Host Discovery Scan**	Finds live devices on a network (ping scan).

✅ **Pro Tip:** Use **"Basic Network Scan"** for a quick security check.

🔹 2. Scheduling Scans in Nessus

Instead of running scans manually, you can schedule them to run **daily, weekly, or monthly**.

🛠️ How to Schedule a Scan:

1️⃣ **Go to "Scans" > Click "New Scan"**
2️⃣ Choose a scan template and configure target hosts
3️⃣ Click **"Schedule"** in the scan settings
4️⃣ Select **Run Frequency:**

- 🕒 **Once** → Runs the scan only one time
- 🔁 **Daily** → Runs every day at a set time
- 📅 **Weekly** → Runs on specific days (e.g., every Monday)
- 🗓️ **Monthly** → Runs on a fixed date each month
  5️⃣ Set the **Start Time** (Choose your preferred time zone)
  6️⃣ Click **"Save"**

✅ **Pro Tip:** Schedule scans **during off-peak hours** to avoid network slowdowns.

🔹 3. Managing Scan Results

Once a scan is complete, you need to **analyze and manage the results** effectively.

🛠️ How to View Scan Results

1️⃣ **Go to "Scans" > Click on a Completed Scan**
2️⃣ View the **summary dashboard**:

- 🟥 **Critical Vulnerabilities (Red)** → Highest risk
- 🟠 **High Vulnerabilities (Orange)** → Severe risk
- 🟡 **Medium Vulnerabilities (Yellow)** → Moderate risk
- 🔵 **Low & Informational (Blue/Gray)** → Minimal impact
  3️⃣ Click on a vulnerability to see:
- **CVE ID** (Common Vulnerability Enumeration)
- **Exploitability Score** (can it be remotely exploited?)
- **Affected Systems**
- **Recommended Fixes**

🛠️ How to Export Scan Reports

1️⃣ Open a **completed scan**
2️⃣ Click **"Export"** (top-right corner)
3️⃣ Choose the format:

- 📄 **PDF** → Management-friendly summary

- 📊 **CSV** → Raw data for analysis
- 📜 **JSON/XML** → For automation tools
  4️⃣ Save and share the report with your security team

✅ **Pro Tip:** Use **CSV exports** for deep analysis in Excel or SIEM tools.

🔹 4. Managing Scan Policies for Optimization

A **Scan Policy** defines how Nessus scans a target. Optimizing scan policies improves performance and accuracy.

🛠️ How to Create a Custom Scan Policy

1️⃣ **Go to "Policies" > Click "New Policy"**
2️⃣ Choose a **Scan Type** (e.g., Network, Web App, Advanced)
3️⃣ Configure:

- **Scan Performance:** Adjust scan depth and speed
- **Safe Checks:** Avoids crashing production systems
- **Credentialed Scanning:** Uses SSH/RDP for deeper analysis
- **Port Scanning:** Controls which ports are checked
  4️⃣ Save the policy and apply it to new scans

✅ **Pro Tip:** Use **Safe Checks** for scanning critical servers **without disruption**.

🔹 5. Automating Scan Management

You can automate scanning and **trigger alerts when vulnerabilities are found**.

🛠️ How to Automate Scanning

1️⃣ **Use Scheduled Scans** → Regularly check for new vulnerabilities
2️⃣ **Enable Notifications** → Get email alerts for scan results
3️⃣ **Integrate with SIEM tools** (e.g., Splunk, ELK) for real-time monitoring

✅ **Pro Tip:** Automate scans on **high-risk assets** (e.g., public-facing servers) **every week**.

🎯 Final Tips for Mastering Nessus Scans

✓ **Use Scheduled Scans** → Automate security checks to detect threats early
✓ **Run Credentialed Scans** → Get deeper vulnerability insights
✓ **Analyze Reports Regularly** → Prioritize fixes based on risk level
✓ **Use Custom Scan Policies** → Optimize scanning for different environments
✓ **Monitor Trends** → Keep track of recurring vulnerabilities